ABSTRACT OF THE DISCLOSURE

An approach for facilitating secure communications among multicast nodes in a telecommunications network is disclosed. A source node sends an encryption key and an identifier to an authoritative node that stores the encryption key and associates the identifier with the encryption key. The source node encrypts data using the encryption key and sends the encrypted data with the identifier in a multicast. The multicast destination nodes retrieve the encryption key from the authoritative node based on the identifier and then decrypt the multicast. A list of administrative nodes, a list of authorized nodes, and an expiration time may be used to manage the encryption key. The authoritative node may be a certificate authority or key distribution center, and the source node may encrypt the multicast using the Internet security protocol (IPsec) or secure socket layer (SSL). Thus, communications among multicast nodes may be efficiently secured in a scalable manner.